桌面管理指南
商用台式机

文档部件号：312947-AA2

2003 年 9 月

本指南介绍了预装在某些机型上的安全保护功能和智能管理功能的定义及使用说明。

警告：以这种方式出现的文字表示如果不按照指示操作，可能会造成人身伤害或带来生命危险。

注意：以这种方式出现的文字表示如果不按照指示操作，可能会损坏设备或丢失信息。

桌面管理指南
商用台式机

第二版 （2003 年 9 月）
文档部件号：312947-AA2

目录

桌面管理指南

索引

桌面管理指南

HP Intelligent Manageability （HP 智能管理）软件针对网络环境中的台式机、工作站以及笔记本个人计算机的管理和控制提供了各种基于标准的解决方案。 HP 于 1995 年推出了业界第一批可全面管理的台式个人计算机，进而成为台式机管理技术的先锋。HP 在管理技术方面拥有专利。从那时起，HP 就领导业界，共同努力制订出有效部署、配置及管理台式机、工作站和笔记本个人计算机所需的标准和基础结构。 HP 与业界主要的管理软件解决方案提供商密切合作，以确保自己的智能管理技术与这些产品相兼容。我们竭力为您提供个人计算机生命周期的解决方案，以此来协助您历经台式个人计算机生命周期的四个阶段 （即计划、部署、管理与过渡），而智能管理正是其中的一个重要组成部分。

桌面管理的主要功能和特点如下：

- 初始配置和部署
- 远程系统安装
- 软件更新和管理
- ROM 快擦写
- 资产跟踪和安全保护
- 故障通知和恢复

对本指南中所述的特定功能的支持可能随机型或软件版本而有所不同。

初始配置和部署

该计算机中配备了预装的系统软件映像。经过简短的软件 “解包”过程之后，就可以使用计算机了。

您可能喜欢使用一套自定义的系统和应用程序软件代替预安装的软件映像。部署自定义软件映像的方法有若干种。其中包括以下几种：

- 将预安装的软件映像解包之后，安装额外的软件应用程序。
- 使用诸如 Altiris Deployment Solution™ 等软件部署工具将预安装的软件替换为自定义的软件映像。
- 使用磁盘克隆方法将内容从一个硬盘驱动器复制到另一个硬盘驱动器中。

您应根据自己的信息技术环境和步骤来选取最佳的部署方法。在 HP 网站的 HP Lifecycle Solutions （生命周期解决方案）(http://h18000.www1.hp.com/solutions/pcsolutions) 中的 PC Deployment （个人计算机部署）部分提供的信息可帮助您选择最佳的部署方法。

Restore Plus! 光盘、基于 ROM 的设置实用程序，以及 ACPI 硬件则更加有助于恢复系统软件、管理配置、排除故障和实施电源管理。

远程系统安装

借助于远程系统安装，您可以启动预引导执行环境 (PXE)，进而使用位于网络服务器上的软件和配置信息来启动和设置系统。远程系统安装功能通常用作系统设置和配置工具，而且可以用来执行以下任务：

- 格式化硬盘驱动器
- 在一台或多台新的个人计算机上部署软件映像
- 远程更新快擦写 ROM 中的系统 BIOS（第 8 页上的“远程 ROM 快擦写”）
- 配置系统 BIOS 设置

要启动远程系统安装，请在 HP 徽标屏幕的右下角出现“F12 = Network Service Boot （网络服务引导）”消息时按下 **F12** 键。随后，请按照屏幕上的说明继续进行操作。默认的引导顺序是一项 BIOS 配置设置，可以将其更改为始终尝试 PXE 引导。

HP 和 Altiris 公司共同合作提供了一些工具，其目的是简化公司部署和管理个人计算机的任务和节省时间，从而最终降低总的拥有成本，并且使 HP 个人计算机成为企业环境中最便于管理的客户机。

软件更新和管理

HP 提供了多种管理和更新台式机和工作站软件的工具，其中包括 Altiris、 Altiris PC Transplant Pro、 HP Client Manager （HP 客户机管理器）软件 （一种 Altiris 解决方案）、 System Software Manager （系统软件管理器）、 HP Proactive Notification （HP 主动通知）和 ActiveUpdate。

HP 客户机管理器软件

智能型 HP Client Manager Software （HP 客户机管理器软件，HP CMS）可与 Altiris 中的 HP Intelligent Manageability （HP 智能管理）技术紧密融合，从而使 HP 的访问设备具有以下各种出色的硬件管理功能：

- 硬件清单的详细视图，便于实施资产管理
- 个人计算机运行状况的监视与诊断
- 主动发出有关硬件环境更改的通知
- 可通过 Web 访问关键业务的详情报告（如发出过热警告的计算机、内存警报等等）
- 远程更新系统软件，如设备驱动程序和 ROM BIOS
- 远程更改引导顺序

有关 HP Client Manager （HP 客户机管理器）的详细信息，请访问 http://h18000.www1.hp.com/im/client_mgr.html。

Altiris 解决方案

利用 HP Client Management Solutions （HP 客户机管理解决方案），可以集中管理处于 IT 生命周期的各个阶段的 HP 客户机设备硬件。

- 清点和管理资产
  - 遵从软件许可要求
  - 个人计算机的跟踪和报告
  - 租赁合同、固定资产跟踪

- 部署与迁移
  - Microsoft Windows 2000、 Windows XP Professional 版或 Windows XP Home 版的迁移
  - 系统部署
  - 个性化迁移
- 服务中心和问题解答
  - 管理服务中心票券
  - 远程排除故障
  - 远程解决问题
  - 客户端灾难恢复
- 软件和运行管理
  - 随时完善的桌面管理
  - HP 系统软件的部署
  - 应用程序的自行修复

在某些型号的台式机和笔记本计算机上， Altiris 管理代理已作为出厂时装载的映像一同提供。有了此代理，就可以和 Altiris Development Solution （Altiris 开发解决方案）进行沟通，利用各种简单明了的向导完成新硬件的部署或者向新的操作系统进行个性化迁移。 Altiris 解决方案具有简单易用的软件分发功能。在与 System Software Manager （系统软件管理器）或 HP Client Manager （HP 客户机管理器）配合使用的情况下，管理员还可以通过中央控制台更新 ROM BIOS 和设备驱动程序软件。

有关详细信息，请访问 http://www.hp.com/go/easydeploy。

Altiris PC Transplant Pro

Altiris PC Transplant Pro 可保留原有设置、首选项和数据。这样一来，用户就可以快捷地将它们迁移到新的环境中，从而毫不费力地完成个人计算机的迁移操作。执行升级操作也只需几分钟的时间，而不必占用几个小时或几天。升级后的台式机完全可以达到用户预期的要求。

有关如何下载功能齐全的 30 天试用版本的详细信息，请访问 http://h18000.www1.hp.com/im/prodinfo.html#deploy。

系统软件管理器

System Software Manager （系统软件管理器， SSM）是一种实用程序，使您可以同时更新多个系统的系统级软件。在个人计算机客户机系统上执行 SSM 时，它将检测硬件和软件的版本，然后通过中央存储库 （也称为文件仓库）更新相应的软件。在驱动程序下载网站和支持软件光盘上，都用特殊的图标表示 SSM 支持的驱动程序版本。要下载该实用程序或了解有关 SSM 的详细信息，请访问 http://h18000.www1.hp.com/im/ssmwp.html。

主动更改通知

Proactive Change Notification （主动更改通知）程序利用订户选择的网站，主动并自动地执行以下操作：

- 通过电子邮件向您发送主动更改通知 (Proactive Change Notification, PCN)，让您提前 60 天获知大多数商用计算机和服务器的软、硬件变更信息。
- 向您发送电子邮件，其中含有与大多数商用计算机和服务器有关的客户公告、客户咨询、客户注释、安全公告，以及驱动程序警报等。

创建自己的配置文件，以确保只接收与特定 IT 环境相关的信息。要了解有关 Proactive Change Notification （主动更改通知）程序的详细信息和创建自定义的配置文件，请访问 http://www.hp.com/go/pcn。

ActiveUpdate

ActiveUpdate 是 HP 提供的基于客户机的应用程序。ActiveUpdate 客户程序在本地系统上运行，并利用用户定义的配置文件主动且自动地下载适用于大多数 HP 商用计算机和服务器的软件更新。 HP Client Manager Software （HP 客户机管理器软件）和 System Software Manager （系统软件管理器）能够以智能方式将这些下载的软件更新部署到目标计算机上。

要了解有关 ActiveUpdate 的详细信息、下载相关的应用程序以及创建自定义的配置文件，请访问 http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html。

ROM 快擦写

该计算机配备了可编程的快擦写 ROM （只读存储器）。要防止意外更新或重写 ROM，只需在 Computer Setup (F10) （计算机设置 (F10)）实用程序中设定设置密码即可。这对于确保计算机操作的完整性十分重要。如果您需要或希望升级 ROM，可以采取以下方法：

- 从 HP 方面订购升级的 ROMPaq 软盘。
- 从 http://h18000.www1.hp.com/im/ssmwp.html 处下载最新的 ROMPaq 映像。

注意：为了最大限度地保护 ROM，请务必设定设置密码。设置密码可以防止他人擅自升级 ROM。有了 System Software Manager （系统软件管理器），系统管理员就可以同时在一台或多台个人计算机上设定设置密码。有关详细信息，请访问 http://h18000.www1.hp.com/im/ssmwp.html。

远程 ROM 快擦写

借助于远程 ROM 快擦写功能，系统管理员可以直接通过中央网络管理控制台安全地对远程 HP 计算机中的 ROM 进行升级。如果系统管理员能够在多台计算机和个人计算机上远程执行此任务，则可以通过网络统一部署 HP PC ROM 映像，并实施更加完善的控制。此外，还可提高工作效率和降低总的拥有成本。

必须接通计算机的电源或者通过远程唤醒功能打开计算机，才能利用远程 ROM 快擦写功能。

有关远程 ROM 快擦写的详细信息，请参阅 http://h18000.www1.hp.com/im/prodinfo.html 处的 HP Client Manager Software （HP 客户机管理器软件）或 System Software Manager （系统软件管理器）。

HPQFlash

利用 HPQFlash 实用程序，可以在本地通过 Windows 操作系统逐一更新或恢复个人计算机中的系统 ROM。

有关 HPQFlash 的详细信息，请访问 http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html。

ROM 防故障引导块

万一发生了 ROM 快擦写故障 （例如， ROM 升级期间出现电源故障），可以利用 ROM 防故障引导块来恢复系统。引导块是 ROM 的快擦写保护区，当接通系统电源后，它将检查系统 ROM 快擦写是否有效。

- 如果系统 ROM 有效，系统将正常启动。
- 如果在检查时发现了系统 ROM 故障， ROM 防故障引导块完全能够通过 ROMPaq 软盘启动系统，利用有效的映象对系统 ROM 进行编程。

如果引导块检测到无效的系统 ROM，系统电源 LED 指示灯便会呈红色闪烁 8 次 （一秒一次），然后暂停 2 秒钟。同时还会听到计算机发出 8 次哔声。屏幕上还将显示引导块恢复模式信息 （仅限于某些机型）。

要在系统进入引导块恢复模式后恢复系统，请执行以下各步操作：

1. 如果软盘驱动器中装有软盘，请取出软盘并关闭电源。
2. 将 ROMPaq 软盘插入软盘驱动器中。
3. 接通系统电源。
4. 如果系统未找到 ROMPaq 软盘，将提示您插入一张 ROMPaq 软盘并重新启动计算机。
5. 如果设定了设置密码， Caps Lock 指示灯将会亮起，而且系统会提示您输入该密码。
6. 输入设置密码。
7. 如果通过该软盘成功地启动了系统并成功地重新编写了 ROM，键盘上的三个指示灯便会亮起。此外，系统还会发出一连串音量逐渐升高的哔声以示大功告成。
8. 取出软盘并关闭电源。
9. 再次接通电源以重新启动计算机。

下表列出了 ROM 引导块所对应的各种键盘指示灯组合 （当 PS/2 键盘与计算机相连时），并解释了每种组合所对应的含义和操作。

ROM 引导块所对应的键盘指示灯组合

防故障引导块模式	键盘 LED 指示灯的颜色	键盘 LED 指示灯的活动	状态/信息
Num Lock	绿色	亮起	ROMPaq 软盘不存在或者已损坏，或者驱动器尚未准备就绪。
Caps Lock	绿色	亮起	输入密码。
Num Lock、Caps Lock、Scroll Lock	绿色	按照下列顺序逐一闪烁 — N、C、 SL	在网络模式下键盘已锁定。
Num Lock、Caps Lock、Scroll Lock	绿色	亮起	ROM 引导块快擦写成功。关闭电源，然后打开电源以重新引导。

USB 键盘上的诊断指示灯不闪烁。

复制设置

系统管理员可按照下列步骤轻松地将一台个人计算机的设置配置复制到相同型号的其它计算机中。这样可以更加迅速、统一地配置多台计算机。

这两个步骤都要用到软盘驱动器或支持的 USB 快擦写介质设备，如 HP Drive Key。

单台复制

注意：设置配置因机型而异。如果源计算机的型号不同于目标计算机的型号，就可能导致文件系统损坏。例如，不要将 D510 超小型台式机的设置配置复制到 D510 e-pc 上。

1. 选择要复制的设置配置。打开或重新启动计算机。如果在 Windows 中，请单击 **Start （开始） > Shut Down （关闭系统） > Restart the Computer （重新启动计算机）**。
2. 当显示器指示灯变成绿色时，立即按下 **F10** 键。您也可以根据需要按下 **Enter** 键跳过标题屏幕。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

3. 插入软盘或 USB 快擦写介质设备。
4. 单击 **File （文件） > Save to Diskette （保存到软盘）**。按照屏幕上的说明进行操作，即可创建配置软盘或 USB 快擦写介质设备。
5. 关闭要配置的计算机，然后插入配置软盘或 USB 快擦写介质设备。
6. 打开要配置的计算机。当显示器指示灯变成绿色时，立即按下 **F10** 键。您也可以根据需要按下 **Enter** 键跳过标题屏幕。
7. 单击 **File （文件） > Restore from Diskette （从软盘恢复）**，然后按照屏幕上的说明进行操作。
8. 配置完毕后，重新启动计算机。

多台复制

注意：设置配置因机型而异。如果源计算机的型号不同于目标计算机的型号，就可能导致文件系统损坏。例如，不要将 D510 超小型台式机的设置配置复制到 D510 e-pc 上。

采用这种方法来准备配置软盘或 USB 快擦写介质设备时，需要的时间稍长，但是向目标计算机复制相关配置时，速度将大大提高。

在 Windows 2000 下不能创建可引导软盘。要进行多台复制或创建可引导 USB 快擦写介质设备，就必须用到可引导软盘。如果不能使用 Windows 9x 或 Windows XP 创建可引导软盘，请改用单台复制方法 （请参阅第 11 页上的 “单台复制”）。

1. 创建可引导软盘或 USB 快擦写介质设备。请参阅第 13 页上的 “可引导软盘”、第 14 页上的 “支持的 USB 快擦写介质设备”或第 17 页上的 “不支持的 USB 快擦写介质设备”。

注意：并非所有的计算机都可以通过 USB 快擦写介质设备引导。如果在 Computer Setup (F10) （计算机设置 (F10)）实用程序的默认引导顺序中， USB 设备列在硬盘驱动器之前，那么该计算机就可以通过 USB 快擦写介质设备引导。否则，必须使用可引导软盘。

2. 选择要复制的设置配置。打开或重新启动计算机。如果在 Windows 中，请单击 **Start （开始） > Shut Down （关闭系统） > Restart the Computer （重新启动计算机）**。
3. 当显示器指示灯变成绿色时，立即按下 **F10** 键。您也可以根据需要按下 **Enter** 键跳过标题屏幕。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

4. 插入可引导软盘或 USB 快擦写介质设备。
5. 单击 **File （文件） > Save to Diskette （保存到软盘）**。按照屏幕上的说明进行操作，即可创建配置软盘或 USB 快擦写介质设备。

6. 下载用于复制设置的 BIOS 实用程序 (repset.exe)，并将其复制到配置软盘或 USB 快擦写介质设备上。在 http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html 处即可找到该实用程序。
7. 在配置软盘或 USB 快擦写介质设备上，创建包含下列命令的 autoexec.bat 文件：

   repset.exe

8. 关闭要配置的计算机。插入配置软盘或 USB 快擦写介质设备，然后打开计算机。此时，配置实用程序便会自动运行。
9. 配置完毕后，重新启动计算机。

创建可引导设备

可引导软盘

这些说明适用于 Windows XP Professional 版和 Windows XP Home 版。在 Windows 2000 下，不能创建可引导软盘。

1. 将软盘插入软盘驱动器。
2. 单击 **Start （开始）**，然后单击 **My Computer （我的电脑）**。
3. 右击软盘驱动器，然后单击 **Format （格式化）**。
4. 选中 **Create an MS-DOS startup disk （创建 MS-DOS 启动磁盘）**复选框，然后单击 **Start （开始）**。

返回第 12 页上的 “多台复制”。

支持的 USB 快擦写介质设备

HP Drive Key 或 DiskOnKey 等支持的设备上已带有预装的映像，从而简化了将其设置为可引导设备的过程。如果所用的 Drive Key 上并没有此映像，请按照本节后面介绍的步骤进行操作 （请参阅第 17 页上的 “不支持的 USB 快擦写介质设备”）。

注意：并非所有的计算机都可以通过 USB 快擦写介质设备引导。如果在 Computer Setup (F10) （计算机设置 (F10)）实用程序的默认引导顺序中， USB 设备列在硬盘驱动器之前，那么该计算机就可以通过 USB 快擦写介质设备引导。否则，必须使用可引导软盘。

要创建可引导 USB 快擦写介质设备，必须具备下列条件：

- 拥有下列某种系统：
  - Compaq Evo D510 超小型台式机
  - Compaq Evo D510 可转换小型立式机型/纤小机型
  - HP Compaq 商用台式机 d530 系列 — 超小型台式机、纤小机型或可转换小型立式机型
  - Compaq Evo N400c、 N410c、 N600c、 N610c、 N620c、 N800c 或 N1000c 笔记本计算机
  - Compaq Presario 1500 或 2800 笔记本计算机

  今后的系统可能还支持引导至 HP Drive Key，具体情况取决于各自的 BIOS。

注意：如果所用的计算机并不是先前提到的计算机，就应确保在 Computer Setup (F10) （计算机设置 (F10)）实用程序的默认引导顺序中， USB 设备是列在硬盘驱动器前面的。

- 使用的是下列某种存储模块：
  - 16MB HP Drive Key
  - 32MB HP Drive Key
  - 32MB DiskOnKey
  - 64MB HP Drive Key

- ❏ 64MB DiskOnKey
- ❏ 128MB HP Drive Key
- ❏ 128MB DiskOnKey

■ 含有 FDISK 和 SYS 程序的可引导 DOS 软盘。如果没有 SYS，可以使用 FORMAT，但 Drive Key 中现有的所有文件便会丢失。

1. 关闭计算机。
2. 将 Drive Key 插入计算机的某个 USB 端口中，然后卸下 USB 软盘驱动器以外的其它所有 USB 存储设备。
3. 将含有 FDISK.COM 以及 SYS.COM 或 FORMAT.COM 的可引导 DOS 软盘插入软盘驱动器，然后启动计算机以引导至该 DOS 软盘。
4. 在 A:\ 提示符下，键入 **FDISK** 并按下 Enter 键，以运行 FDISK。如果出现提示，请单击 **Yes （是） (Y)**，以便能够支持大容量磁盘。
5. 输入选项 [**5**]，显示系统中的驱动器。 Drive Key 的容量应该最接近于所列的某种驱动器的容量。它通常是列表中的最后一个驱动器。记下该驱动器的盘符。

   Drive Key 驱动器：_____

△ **注意**：如果没有与 Drive Key 相符的驱动器，请不要继续进行操作。否则的话，会丢失数据。检查所有的 USB 端口上是否连有其它的存储设备。如果发现了其它的 USB 设备，请将其卸下，然后重新引导计算机，并从第 4 步开始继续进行操作。如果没有此类设备，则说明该系统不支持 Drive Key 或者 Drive Key 有缺陷。在这种情况下，**不要**继续尝试将 Drive Key 设置为可引导设备。

6. 按 **Esc** 键，退出 FDISK 并返回到 A:\ 提示符下。
7. 如果可引导 DOS 软盘中含有 SYS.COM，请转至步骤 8。否则，转至步骤 9。
8. 在 A:\ 提示符下，输入 **SYS x:** 其中， x 代表先前记下的驱动器盘符。然后，转至步骤 13。

注意：确保已输入的 Drive Key 驱动器的盘符准确无误。

将系统文件传输完毕后， SYS 将返回到 A:\ 提示符下。

9. 将需要保存的所有文件从 Drive Key 复制到其它驱动器 （如系统内部的硬盘驱动器）的临时目录中。
10. 在 A:\ 提示符下，输入 **FORMAT /S X:** 其中， X 代表先前记下的驱动器盘符。

注意：确保已输入的 Drive Key 驱动器的盘符准确无误。

FORMAT 将显示一个或多个警告，并且每次显示警告时都会询问您是否继续进行操作。每次询问时都输入 **y**。
FORMAT 将格式化 Drive Key、添加系统文件并要求输入卷标。

11. 如果不需要卷标，则按 **Enter** 键；如果需要，则输入卷标。
12. 将在执行第 9 步操作时保存的所有文件重新复制到 Drive Key 中。
13. 取出软盘，然后重新引导计算机。计算机将引导至作为驱动器 C 的 Drive Key。

计算机的默认引导顺序因计算机而异，在 Computer Setup (F10)（计算机设置 (F10)）实用程序中可以更改该顺序。

如果是在 Windows 9x 中使用 DOS 版本，屏幕上可能短暂显示 Windows 徽标。如果不希望看到此屏幕，请在 Drive Key 的根目录下添加长度为零的 LOGO.SYS 文件。

返回第 12 页上的 “多台复制”。

不支持的 USB 快擦写介质设备

注意：并非所有的计算机都可以通过 USB 快擦写介质设备引导。如果在 Computer Setup (F10)（计算机设置 (F10)）实用程序的默认引导顺序中，USB 设备列在硬盘驱动器之前，那么该计算机就可以通过 USB 快擦写介质设备引导。否则，必须使用可引导软盘。

要创建可引导 USB 快擦写介质设备，必须具备下列条件：

- 拥有下列某种系统：
  - Compaq Evo D510 超小型台式机
  - Compaq Evo D510 可转换小型立式机型/纤小机型
  - HP Compaq 商用台式机 d530 系列 — 超小型台式机、纤小机型或可转换小型立式机型
  - Compaq Evo N400c、 N410c、 N600c、 N610c、 N620c、 N800c 或 N1000c 笔记本计算机
  - Compaq Presario 1500 或 2800 笔记本计算机

  今后的系统可能还支持引导至 USB 快擦写介质设备，具体情况取决于各自的 BIOS。

注意：如果所用的计算机并不是先前提到的计算机，就应确保在 Computer Setup (F10)（计算机设置 (F10)）实用程序的默认引导顺序中，USB 设备是列在硬盘驱动器前面的。

- 含有 FDISK 和 SYS 程序的可引导 DOS 软盘。如果没有 SYS，可以使用 FORMAT，但 Drive Key 中现有的所有文件便会丢失。

1. 如果系统中的任何 PCI 卡上连有 SCSI、 ATA RAID 或 SATA 驱动器，请关闭计算机并拔出电源线插头。

注意：必须拔出电源线插头。

2. 打开计算机，并卸下 PCI 卡。
3. 将 USB 快擦写介质设备插入计算机的某个 USB 端口中，然后卸下 USB 软盘驱动器以外的其它所有 USB 存储设备。合上计算机盖板。

4. 插入电源线插头，然后打开计算机。当显示器的指示灯变成绿色时，立即按下 **F10** 键，进入计算机设置实用程序。
5. 转至 Advanced/PCI （高级/PCI）处，禁用 IDE 和 SATA 控制器。禁用 SATA 控制器后，记下控制器被分配给哪个 IRQ。以后需要重新分配 IRQ。退出计算机设置实用程序，确认所做更改。

   SATA IRQ: _____

6. 将含有 FDISK.COM 以及 SYS.COM 或 FORMAT.COM 的可引导 DOS 软盘插入软盘驱动器，然后启动计算机以引导至该 DOS 软盘。
7. 运行 FDISK，并删除 USB 快擦写介质设备上所有的现有分区。创建一个新的分区，并将其标为活动分区。按 **Esc** 键退出 FDISK。
8. 如果退出 FDISK 后，系统并未自动重启，请按 **Ctrl**+**Alt**+**Del** 键，重新引导至 DOS 软盘。
9. 在 A:\ 提示符下，键入 **FORMAT C:/S**，然后按 **Enter** 键。FORMAT 将格式化 USB 快擦写介质设备、添加系统文件并要求输入卷标。
10. 如果不需要卷标，则按 **Enter** 键；如果需要，则输入卷标。
11. 关闭计算机，然后拔下电源线插头。拆开计算机，重新安装先前卸下的所有 PCI 卡。合上计算机盖板。
12. 插入计算机电源线插头，取出软盘，然后打开计算机。
13. 当显示器指示灯变成绿色时，立即按下 **F10** 键，进入计算机设置实用程序。
14. 转至 Advanced/PCI Devices （高级/PCI 设备），并重新启用在第 5 步中禁用的 IDE 和 SATA 控制器。将原有的 IRQ 分配给 SATA 控制器。
15. 保存更改并退出。计算机将引导至作为驱动器 C 的 USB 快擦写介质设备。

计算机的默认引导顺序因计算机而异，在 Computer Setup (F10)（计算机设置 (F10)）实用程序中可以更改该顺序。

如果是在 Windows 9x 中使用 DOS 版本，屏幕上可能短暂显示 Windows 徽标。如果不希望看到此屏幕，请在 Drive Key 的根目录下添加长度为零的 LOGO.SYS 文件。

返回第 12 页上的 “多台复制”。

双重状态电源按钮

如果在 Windows 2000、 Windows XP Professional 版和 Windows XP Home 版中启用了高级配置和电源接口 (ACPI)，电源按钮就可以用作打开/关闭开关或挂起按钮。挂起功能并不能彻底关闭电源，只是使计算机进入低功耗的等待状态而已。这样一来，您不仅可以快速关机且无需关闭应用程序，而且可以快速返回到原来的操作状态而不会丢失任何数据。

要更改电源按钮的配置，请完成以下各步操作：

1. 在 Windows 2000 中，左击 **Start （开始）**按钮，然后选择 **Settings （设置） > Control Panel （控制面板） > Power Options （电源选项）**。

   在 Windows XP Professional 版和 Windows XP Home 版中，左击 **Start （开始）**按钮，然后选择 **Control Panel （控制面板） > Performance and Maintenance （性能和维护） > Power Options （电源选项）**。

2. 在 **Power Options Properties （电源选项属性）**中，选择 **Advanced （高级）**标签。

3. 在 **Power Button （电源按钮）**部分，选择所需的电源按钮设置。

在将电源按钮配置成挂起按钮之后，按下电源按钮将系统置入低功耗的状态 （挂起）。再次按下此按钮，可快速将系统从挂起状态恢复到全功耗状态。要彻底关闭系统电源，请持续按住电源按钮 4 秒钟。

注意：请勿使用电源按钮关闭计算机，除非系统不响应；如果不通过操作系统关闭电源，可能会损坏硬盘驱动器或丢失硬盘驱动器中的数据。

万维网站

HP 工程师不仅对 HP 及第三方供应商开发的软件进行极为严格的测试与调试，而且还开发适用于特定操作系统的支持软件，以确保 HP 个人计算机的性能、兼容性和可靠性。

如果要改用新版或修订版的操作系统，请务必采用专门适用于该操作系统的支持软件。如果准备运行的 Microsoft Windows 的版本不同于计算机中装有的版本，就必须安装相应的设备驱动程序和实用程序，以确保支持所有的功能，而且能够让它们正常地发挥作用。

HP 简化了查找、访问、评估和安装最新支持软件的操作。您可以通过 http://www.hp.com/support 下载该软件。

该网站上提供了在 HP 计算机上运行最新的 Microsoft Windows 操作系统所需的最新的设备驱动程序、实用程序和可快擦写的 ROM 映像。

积木式组件和伙伴

HP 管理解决方案不仅融合了其它系统的管理应用程序，而且还以下列业界标准为基准：

- 桌面管理接口 (DMI) 2.0
- 局域网唤醒技术
- ACPI
- SMBIOS
- 预引导执行 (PXE) 支持

资产跟踪和安全保护

本计算机还具备资产跟踪功能，您可以利用 HP Insight Manager（HP 洞察管理器）、 HP Client Manager （HP 客户机管理器）或其它系统管理应用程序进行数据管理。由于资产跟踪功能可以自动与这些产品进行完美融合，因此您可以根据环境来选择最适当的管理工具，并充分发挥现有工具的投资效益。

HP 还提供了几种用来控制访问重要组件和信息的方法。如果安装了 ProtectTools Embedded Security （ProtectTools 嵌入式安全保护）装置，还可以防止他人擅自访问数据，并检查系统完整性，还可以对尝试访问系统的第三方用户进行验证。某些机型还具备安全保护功能，例如 ProtectTools、智能机盖传感器和智能机盖锁，以防止他人擅自接触个人计算机的内部组件。通过禁用并行、串行或 USB 端口，或者禁用可拆卸介质引导功能，您可以保护重要的数据资产。内存更改警报和智能机盖传感器警报都可以自动转发到系统管理应用程序中，如果窜改了计算机的内部组件，系统便会主动发出通知。

只有某些系统提供 Protect Tools、智能机盖传感器和智能机盖锁等选件。

利用下列实用程序，可管理 HP 计算机上的安全保护设置：

- 在本地运行 Computer Setup （计算机设置）实用程序。有关使用 Computer Setup （计算机设置）实用程序的额外信息和说明，请参阅随机附带的*计算机设置 (F10) 实用程序指南*。
- 远程使用 HP Client Manager （HP 客户机管理器）或 System Software Manager （系统软件管理器）。利用上述软件，可通过简单的命令行实用程序安全、统一地部署和控制安全保护设置。

在下表及各小节中，将介绍有关通过 Computer Setup (F10) （计算机设置 (F10)）实用程序从本地管理计算机的安全保护功能的信息。

安全保护功能概述

功能	用途	设置方式
可拆卸介质引导控制	防止从可拆卸介质驱动器引导。（适用于某些驱动器）	利用计算机设置 (F10) 实用程序菜单。
串行接口、并行接口、USB 接口或红外接口控制	防止通过集成的串行接口、并行接口或 USB （通用串行总线）接口或红外接口传输数据。	利用计算机设置 (F10) 实用程序菜单。
开机密码	必须输入该密码才能使用计算机。系统初次启动和重新启动时都必须输入该密码。	利用计算机设置 (F10) 实用程序菜单。
设置密码	必须输入该密码，才能使用 Computer Setup （计算机设置）实用程序重新配置计算机。	利用计算机设置 (F10) 实用程序菜单。
嵌入式安全保护设备	采取加密和密码保护措施，以防他人擅自访问数据。检查系统的完整性，并对尝试访问系统的第三方用户进行验证。	利用计算机设置 (F10) 实用程序菜单。
驱动器锁	防止他人擅自访问多功能插槽硬盘驱动器上的数据。只有某些机型才具备该功能。	利用计算机设置 (F10) 实用程序菜单。

有关 Computer Setup （计算机设置）实用程序的详细信息，请参阅 *计算机设置 (F10) 实用程序指南*。

所支持的安全保护功能可能因计算机的具体配置而异。

安全保护功能概述 *（续）*

功能	用途	设置方式
智能机盖传感器	表明计算机的机盖或侧面板是否曾被卸下。可以对智能机盖传感器进行设置，一旦卸下机盖或侧面板，就必须输入设置密码才能重新启动计算机。有关此功能的详细信息，请参阅 *文档库* 光盘中的 *硬件参考指南*。只有某些机型才具备该功能。	利用计算机设置 (F10) 实用程序菜单。
主引导记录安全保护	防止无意或恶意更改当前可引导盘上的主引导记录，并提供一种恢复 “最新最全” 的主引导记录的方法。	利用计算机设置 (F10) 实用程序菜单。
内存更改警报	一旦添加、移动或卸下了内存模块，就能检测到相关情况，并通知用户和系统管理员。	有关启用内存更改警报的信息，请参阅联机 *智能管理指南*。
物主标签	在系统启动 （受设置密码保护）期间，显示由系统管理员定义的物主信息。	利用计算机设置 (F10) 实用程序菜单。
缆锁装置	禁止他人接触计算机内部，以防更改系统配置或拆卸组件。还可以将计算机固定到某一固定物体上，以防被盗。	安装缆锁，以便将计算机固定到某一固定物体上。
防盗环装置	禁止他人接触计算机内部，以防更改系统配置或拆卸组件。	给防盗环上锁，以防他人更改系统配置或拆卸内部组件。

有关 Computer Setup （计算机设置）实用程序的详细信息，请参阅 *计算机设置 (F10) 实用程序指南*。

所支持的安全保护功能可能因计算机的具体配置而异。

密码安全保护

开机密码可用来防止他人擅自使用计算机，因为每当用户开启或重新启动计算机时都必须输入该密码方可访问应用程序或数据。设置密码则专门用来防止他人擅自访问 Computer Setup（计算机设置）实用程序，而且它还可以代替开机密码。也就是说，当系统提示输入开机密码时，输入设置密码也可以访问该计算机。

此外，还可以设定网络范围的设置密码。这样一来，系统管理员无需知道开机密码就可以登录到所有的网络系统来执行维护操作 （即使已经设定了开机密码也无妨）。

利用计算机设置实用程序设定设置密码

如果系统配备了嵌入式安全保护设备，请参阅第 29 页上的 “嵌入式安全保护”。

如果利用 Computer Setup （计算机设置）实用程序设定了设置密码，就必须输入该密码才能使用 Computer Setup (F10) （计算机设置 (F10)）实用程序重新配置计算机。

1. 打开或重新启动计算机。如果在 Windows 中，请单击 **Start（开始） > Shut Down （关闭系统） > Restart the Computer（重新启动计算机）**。
2. 当显示器指示灯变成绿色时，立即按下 **F10** 键。您也可以根据需要按下 **Enter** 键跳过标题屏幕。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

3. 选择 **Security （安全保护）**，然后选择 **Setup Password （设置密码）**，并按照屏幕上的说明进行操作。
4. 在退出之前，请单击 **File （文件） > Save Changes and Exit（保存更改并退出）**。

利用计算机设置实用程序设定开机密码

如果利用 Computer Setup （计算机设置）实用程序设定了开机密码，那么当接通计算机的电源后，就必须输入该密码才能对其进行访问。如果设定了开机密码， Computer Setup （计算机设置）实用程序的 Security （安全保护）菜单中便会出现 Password Options （密码选项）。 Password options （密码选项）包括 Password Prompt on Warm Boot （热启动时提示密码）。如果启用了 Password Prompt on Warm Boot （热启动时提示密码）选项，那么每当重新引导计算机时都必须输入密码。

1. 打开或重新启动计算机。如果在 Windows 中，请单击 **Start （开始） > Shut Down （关闭系统） > Restart the Computer （重新启动计算机）**。
2. 当显示器指示灯变成绿色时，立即按下 **F10** 键。您也可以根据需要按下 **Enter** 键跳过标题屏幕。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

3. 选择 **Security （安全保护）**，然后选择 **Power-On Password （开机密码）**，并按照屏幕上的说明进行操作。
4. 在退出之前，请单击 **File （文件） > Save Changes and Exit （保存更改并退出）**。

输入开机密码

要输入开机密码，请完成以下各步操作：

1. 打开或重新启动计算机。如果在 Windows 中，请单击 **Start （开始） > Shut Down （关闭系统） > Restart the Computer （重新启动计算机）**。
2. 当显示器上出现钥匙图标时，键入当前的密码，然后按下 **Enter** 键。

键入密码时，请小心谨慎；为了安全起见，您所键入的字符不会显示在屏幕上。

如果您输入的密码不正确，屏幕将显示断开的钥匙图标。请再次输入密码。如果三次输入的密码都不正确，就必须关闭计算机，然后再打开才能继续进行输入。

输入设置密码

如果系统配备了嵌入式安全保护设备，请参阅第 29 页上的 “嵌入式安全保护”。

如果在计算机中设定了设置密码，那么每当运行 Computer Setup（计算机设置）实用程序时都会提示您输入该密码。

1. 打开或重新启动计算机。如果在 Windows 中，请单击 **Start（开始） > Shut Down （关闭系统） > Restart the Computer（重新启动计算机）**。
2. 当显示器指示灯变成绿色时，立即按下 **F10** 键。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

3. 当显示器上出现钥匙图标时，键入设置密码，然后按 **Enter** 键。

键入密码时，请小心谨慎；为了安全起见，您所键入的字符不会显示在屏幕上。

如果您输入的密码不正确，屏幕将显示断开的钥匙图标。请再次输入密码。如果三次输入的密码都不正确，就必须关闭计算机，然后再打开才能继续进行输入。

更改开机密码或设置密码

如果系统配备了嵌入式安全保护设备，请参阅第 29 页上的 “嵌入式安全保护”。

1. 打开或重新启动计算机。如果在 Windows 中，请单击 **Start（开始） > Shut Down （关闭系统） > Restart the Computer（重新启动计算机）**。要更改设置密码，请运行 **Computer Setup （计算机设置）**实用程序。
2. 当屏幕上出现钥匙图标时，依次键入当前密码、一条斜杠 (/) 或备选分隔符、新密码、另一条斜杠 (/) 或备选分隔符和新密码 （如下所示）：
   当前密码/新密码/新密码

键入密码时，请小心谨慎；为了安全起见，您所键入的字符不会显示在屏幕上。

3. 按下 **Enter** 键。

在下次打开计算机时，新的密码便会生效。

有关备选分隔符的信息，请参阅第 28 页上的 “国家级键盘分隔符”。您还可以使用 Computer Setup （计算机设置）实用程序中的 Security （安全保护）选项来更改开机密码和设置密码。

删除开机密码或设置密码

如果系统配备了嵌入式安全保护设备，请参阅第 29 页上的 “嵌入式安全保护”。

1. 打开或重新启动计算机。如果在 Windows 中，请单击 **Start（开始） > Shut Down （关闭系统） > Restart the Computer（重新启动计算机）**。要删除设置密码，请运行 **Computer Setup （计算机设置）**实用程序。
2. 当屏幕上出现钥匙图标时，键入当前密码，然后键入斜杠 (/) 或其它分隔符 （如下所示）：
   当前密码/
3. 按下 **Enter** 键。

有关备选分隔符的信息，请参阅 “国家级键盘分隔符”。您还可以使用 Computer Setup （计算机设置）实用程序中的 Security（安全保护）选项来更改开机密码和设置密码。

国家级键盘分隔符

每种键盘的设计均符合特定国家/地区的要求。更改或删除密码所用的语法和按键要视计算机附带的键盘而定。

国家级键盘分隔符

BHCSY*	-	韩语	/	斯洛伐克语	-
阿拉伯语	/	加拿大法语	é	泰语	/
巴西语	/	捷克语	-	土耳其语	.
比利时语	=	拉美语	-	西班牙语	-
波兰语	-	美国英语	/	希伯莱语	.
丹麦语	-	挪威语	-	希腊语	-
德语	-	葡萄牙语	-	匈牙利语	-
俄语	/	日语	/	意大利语	-
法语	!	瑞典语/芬兰语	/	英国英语	/
繁体中文	/	瑞士语	-	中文	/

* 代表波斯尼亚–黑塞哥维纳、克罗地亚、斯洛文尼亚和南斯拉夫

清除密码

如果忘记了密码，则无法访问计算机。有关清除密码的说明，请参阅*故障排除指南*。

如果系统配备了嵌入式安全保护设备，请参阅 “嵌入式安全保护”。

嵌入式安全保护

ProtectTools Embedded Security （ProtectTools 嵌入式安全保护）装置结合了加密和密码保护措施，可确保嵌入式文件系统 (EFS) 文件/文件夹加密和 Microsoft Outlook 及 Outlook Express 电子邮件的安全。在某些商用台式机上， ProtectTools 可作为订购配置 (Configured-To-Order, CTO) 选件提供。该选件是为那些关注数据安全的 HP 客户提供的：擅自访问数据的危险远远超出数据损失的危险。 ProtectTools 使用四种密码：

- (F10) Setup （计算机设置）实用程序 — 进入 Computer Setup （计算机设置 (F10)）实用程序，并启用/禁用 ProtectTools
- Take Ownership （成为物主）— 由系统管理员设置和使用，管理员将对用户进行授权并设置安全保护参数
- Emergency Recovery Token （紧急恢复令牌）— 由系统管理员设置，万一计算机或 ProtectTools 芯片出现故障，可用它来进行恢复
- Basic User （基本用户）— 由最终用户设置和使用

如果最终用户的密码丢失了，就无法恢复加密数据。因此，在公司信息系统上复制用户驱动器中含有的数据或者定期备份时，使用 ProtectTools 最安全。

ProtectTools Embedded Security （ProtectTools 嵌入式安全保护）芯片符合 TCPA 1.1 安全保护标准，可以装在某些商用台式机的主板上。每个 ProtectTools 嵌入式安全保护芯片都是唯一的，只能用在特定的计算机上。每个芯片都单独实施密钥保护措施，与其它的计算机组件 （如处理器、内存或操作系统）无关。

支持 ProtectTools Embedded Security （ProtectTools 嵌入式安全保护）的计算机完善并增强了 Microsoft Windows 2000、Windows XP Professional 版或 Windows XP Home 版中原有的安全保护功能。例如，当操作系统可以根据 EFS 来加密本地文件和文件夹时， ProtectTools Embedded Security （ProtectTools 嵌入式安全保护）装置可同时根据平台的根密钥 （存储在硅片中）创建加密密钥，从而提供了额外的安全保护层。此过程称为“封装”加密密钥。 ProtectTools 并不能阻止通过网络来访问未安装 ProtectTools 的计算机。

ProtectTools Embedded Security （ProtectTools 嵌入式安全保护）的主要功能包括：

- 平台验证
- 存储保护
- 数据完整性

注意：保护密码。**没有这些密码，就不能访问或恢复加密数据**。

设置密码

设置

使用 F10 setup （计算机设置）实用程序，可以设定设置密码和启用嵌入式安全保护设备。

1. 当显示器指示灯变成绿色时，立即按下 **F10** 键。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

2. 使用上箭头键或下箭头键选择一种语言，然后按 **Enter** 键。
3. 使用左箭头键或右箭头键移到 **Security （安全保护）**标签上，然后使用上箭头键或下箭头键移 **Setup Password （设置密码）**选项处。按 **Enter** 键。

4. 键入并确认密码。按 **F10** 键，即可接受密码。

键入密码时，请小心谨慎；为了安全起见，键入的字符不会显示在屏幕上。

5. 使用上箭头键或下箭头键移至 **Embedded Security Device（嵌入式安全保护设备）**选项处。按 **Enter** 键。
6. 如果对话框中的选项是 **Embedded Security Device—Disable（嵌入式安全保护设备 — 禁用）**，请使用左箭头键或右箭头键将其更改为 **Embedded Security Device—Enable （嵌入式安全保护设备 — 启用）**。按 **F10** 键，即可接受更改。

注意：如果选中 **Reset to Factory Settings—Reset （重置为出厂设置 — 重置）**选项，将清除所有密钥。*除非* 已备份了相关密钥，否则无法恢复加密数据。（请参阅 “成为物主和紧急恢复令牌”）。只有步骤中要求重置时，才选择 **Reset （重置）**来恢复加密数据 （请参阅第 34 页上的 “恢复加密数据”）。

7. 使用左箭头键或右箭头键移至 **File （文件）**处。使用上箭头键或下箭头键移至 **Save Changes and Exit （保存更改并退出）**选项处。按 **Enter** 键，然后按 **F10** 键进行确认。

成为物主和紧急恢复令牌

必须使用 Take Ownership （成为物主）密码，才能启用或禁用安全保护平台和对用户进行授权。如果嵌入式安全保护设备出现故障，可利用紧急恢复机制对用户进行授权，使其能够访问数据。

1. 如果使用的是 Windows XP Professional 版或 Windows XP Home 版，请单击 **Start （开始） > All Programs （所有程序） > HP ProtectTools Embedded Security Tools （HP ProtectTools 嵌入式安全保护工具） > Embedded Security Initialization Wizard （嵌入式安全保护初始化向导）**。

   如果使用的是 Windows 2000，请单击 **Start （开始） > Programs （程序） > HP ProtectTools Embedded Security Tools （HP ProtectTools 嵌入式安全保护工具） > Embedded Security Initialization Wizard （嵌入式安全保护初始化向导）**。

2. 单击 **Next （下一步）**。
3. 键入并确认 Take Ownership （成为物主）密码，然后单击 **Next （下一步）**。

键入密码时，请小心谨慎；为了安全起见，键入的字符不会显示在屏幕上。

4. 单击 **Next （下一步）**，接受恢复档案所对应的默认位置。
5. 键入并确认 Emergency Recovery Token （紧急恢复令牌）密码，然后单击 **Next （下一步）**。
6. 插入存有 Emergency Recovery Token Key （紧急恢复令牌密钥）的软盘。单击 **Browse （浏览）**，然后选中该软盘。

注意：万一计算机或嵌入式安全保护芯片出现故障，可以使用 Emergency Recovery Token（紧急恢复令牌）密钥来恢复加密数据。**没有该密钥，就不能恢复加密数据**。如果没有 Basic User（基本用户）密码，也无法访问加密数据。请将该软盘放在安全的地方。

7. 单击 **Save （保存）**接受该位置和默认文件名，然后单击 **Next （下一步）**。
8. 单击 **Next （下一步）**，在初始化安全保护平台前确认设置。

有可能显示这样一则消息，指出嵌入式安全保护功能尚未进行初始化。不要单击这则消息；稍后将对此进行解释，而且该消息将在几秒钟后消失。

9. 单击 **Next （下一步）**跳过配置本地策略的步骤。
10. 确保已选中 Start Embedded Security User Initialization Wizard （启动嵌入式安全保护用户初始化向导）复选框，然后单击 **Finish （完成）**。

此时， User Initialization Wizard （用户初始化向导）将自动启动。

基本用户

在用户初始化过程中，将创建 Basic User （基本用户）密码。输入和访问加密数据时必须输入该密码。

注意：保护 Basic User （基本用户）密码。**没有此密码，就不能访问或恢复加密数据**。

1. 如果 User Initialization Wizard （用户初始化向导）尚未打开，请根据下列具体情况执行相应的操作：

   如果使用的是 Windows XP Professional 版或 Windows XP Home 版，请单击 **Start （开始） > All Programs （所有程序） > HP ProtectTools Embedded Security Tools （HP ProtectTools 嵌入式安全保护工具） > User Initialization Wizard （用户初始化向导）**。

   如果使用的是 Windows 2000，请单击 **Start （开始） > Programs （程序） > HP ProtectTools Embedded Security Tools （HP ProtectTools 嵌入式安全保护工具） > User Initialization Wizard （用户初始化向导）**。

2. 单击 **Next （下一步）**。
3. 键入并确认 Basic User Key （基本用户密钥）密码，然后单击 **Next （下一步）**。

键入密码时，请小心谨慎；为了安全起见，键入的字符不会显示在屏幕上。

4. 单击 **Next （下一步）**确认设置。
5. 选择适当的安全保护功能，然后单击 **Next （下一步）**。
6. 单击适当的电子邮件客户端，将其选中后单击 **Next （下一步）**。
7. 单击 **Next （下一步）**，应用加密证书。
8. 单击 **Next （下一步）**确认设置。
9. 单击 **Finish （完成）**。
10. 重新启动计算机。

恢复加密数据

要在更换 ProtectTools 芯片后恢复数据，必须了解以下内容：

- SPEmRecToken.xml — 紧急恢复令牌密钥
- SPEmRecArchive.xml — 隐含文件夹，其默认位置如下：C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- ProtectTools 密码
  - 计算机设置实用程序
  - Take Ownership （成为物主）密码
  - Emergency Recovery Token （紧急恢复令牌）密码
  - Basic User （基本用户）密码

1. 重新启动计算机。
2. 当显示器指示灯变成绿色时，立即按下 **F10** 键。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

3. 键入设置密码，然后按 **Enter** 键。
4. 使用上箭头键或下箭头键选择一种语言，然后按 **Enter** 键。
5. 使用左箭头键或右箭头键移到 **Security （安全保护）**标签上，然后使用上箭头键或下箭头键移至 **Embedded Security Device （嵌入式安全保护设备）**选项处。按 **Enter** 键。
6. 如果只能使用 **Embedded Security Device—Disable （嵌入式安全保护设备 — 禁用）**选项，请执行以下操作：
   a. 使用左箭头键或右箭头键移至 **Embedded Security Device—Enable （嵌入式安全保护设备 — 启用）**选项处。按下 **F10** 键，即可接受更改。
   b. 使用左箭头键或右箭头键移至 **File （文件）**处。使用上箭头键或下箭头键移至 **Save Changes and Exit （保存更改并退出）**选项处。按 **Enter** 键，然后按 **F10** 键进行确认。

c. 转至步骤 1。

如果两个选项都可以使用，请转到步骤 7。

7. 使用上箭头键或下箭头键移至 **Reset to Factory Settings—Do Not Reset （重置为出厂设置 — 不重置）**选项处。立即按下左箭头键或右箭头键。

   此时，将显示一则消息，指明下列情形：如果在退出时保存了设置，那么执行此操作后，嵌入式安全保护设备就会重置为出厂设置。按任意键继续。

   按 **Enter** 键。

8. 作出上述选择后，会立即显示 **Reset to Factory Settings—Reset （重置为出厂设置 — 重置）**选项。按 **F10** 键，即可接受更改。

9. 使用左箭头键或右箭头键移到 **File （文件）**。使用上箭头键或下箭头键移到 **Save Changes and Exit （保存更改并退出）**。按 **Enter** 键，然后按 **F10** 键进行确认。

10. 重新启动计算机。

11. 当显示器指示灯变成绿色时，立即按下 **F10** 键。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

12. 键入设置密码，然后按 **Enter** 键。

13. 使用上箭头键或下箭头键选择一种语言，然后按 **Enter** 键。

14. 使用左箭头键或右箭头键移到 **Security （安全保护）**标签上，然后使用上箭头键或下箭头键移至 **Embedded Security Device （嵌入式安全保护设备）**选项处。按 **Enter** 键。

15. 如果对话框中的选项是 **Embedded Security Device—Disable （嵌入式安全保护设备 — 禁用）**，请使用左箭头键或右箭头键将其更改为 **Embedded Security Device—Enable （嵌入式安全保护设备 — 启用）**。按 **F10** 键。

16. 使用左箭头键或右箭头键移至 **File （文件）**处。使用上箭头键或下箭头键移至 **Save Changes and Exit （保存更改并退出）**选项处。按 **Enter** 键，然后按 **F10** 键进行确认。

17. Windows 打开后，根据下列具体情况执行相应的操作：

    如果使用的是 Windows XP Professional 版或 Windows XP Home 版，请单击 **Start （开始） > All Programs （所有程序） > HP ProtectTools Embedded Security Tools （HP ProtectTools 嵌入式安全保护工具） > Embedded Security Initialization Wizard （嵌入式安全保护初始化向导）**。

    如果使用的是 Windows 2000，请单击 **Start （开始） > Programs （程序） > HP ProtectTools Embedded Security Tools （HP ProtectTools 嵌入式安全保护工具） > Embedded Security Initialization Wizard （嵌入式安全保护初始化向导）**。

18. 单击 **Next （下一步）**。
19. 键入并确认 Take Ownership （成为物主）密码。单击 **Next （下一步）**。

键入密码时，请小心谨慎；为了安全起见，键入的字符不会显示在屏幕上。

20. 请确保已选中 Create a new recovery archive （创建新的恢复档案）。在 **Recovery archive location （恢复档案位置）**下，单击 **Browse （浏览）**。
21. 请不要接受默认的文件名。键入新的文件名，以免替换原文件。
22. 单击 **Save （保存）**，然后单击 **Next （下一步）**。
23. 键入并确认 Emergency Recovery Token （紧急恢复令牌）密码，然后单击 **Next （下一步）**。
24. 插入存有 Emergency Recovery Token Key （紧急恢复令牌密钥）的软盘。单击 **Browse （浏览）**，然后选中该软盘。
25. 请不要接受默认的密钥名。键入新的密钥名，以免替换原密钥。
26. 单击 **Save （保存）**，然后单击 **Next （下一步）**。
27. 单击 **Next （下一步）**，在初始化安全保护平台前确认设置。

有可能出现这样一则消息，指出无法加载 Basic User Key （基本用户密钥）。不要单击这则消息；稍后将对此进行解释，而且该消息将在几秒钟后消失。

28. 单击 **Next （下一步）**跳过配置本地策略的步骤。
29. 单击以清除 **Start Embedded Security User Initialization Wizard （启动嵌入式安全保护用户初始化向导）**复选框。单击 **Finish （完成）**。
30. 在工具栏中右击 ProtectTools 图标，然后单击 **Initialize Embedded Security restoration （初始化嵌入式安全保护恢复）**。

    此操作将启动 HP ProtectTools 嵌入式安全保护初始化向导。
31. 单击 **Next （下一步）**。
32. 插入存有原来的紧急恢复令牌密钥的软盘。单击 **Browse （浏览）**，然后找到并双击该令牌，即可在相应的字段中输入其名称。默认值为 A:\SPEmRecToken.xml。
33. 键入原来的令牌密码，然后单击 **Next （下一步）**。
34. 单击 **Browse （浏览）**，然后找到并双击原来的恢复档案，即可在相应的字段中输入其名称。默认值为 C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml。
35. 单击 **Next （下一步）**。
36. 单击要恢复的计算机，然后单击 **Next （下一步）**。
37. 单击 **Next （下一步）**确认设置。
38. 如果向导指出已经恢复了安全保护平台，请转至步骤 39。

    如果向导指出恢复失败，请退至步骤 10。请仔细检查密码、令牌位置和名称，以及档案的位置和名称。
39. 单击 **Finish （完成）**。

40. 如果使用的是 Windows XP Professional 版或 Windows XP Home 版，请单击 **Start （开始） > All Programs （所有程序） > HP ProtectTools Embedded Security Tools （HP ProtectTools 嵌入式安全保护工具） > User Initialization Wizard （用户初始化向导）**。

    如果使用的是 Windows 2000，请单击 **Start （开始） > Programs （程序） > HP ProtectTools Embedded Security Tools （HP ProtectTools 嵌入式安全保护工具） > User Initialization Wizard （用户初始化向导）**。

41. 单击 **Next （下一步）**。
42. 单击 **Recover your basic user key （恢复基本用户密钥）**，然后单击 **Next （下一步）**。
43. 选择一个用户，键入该用户原来的 Basic User Key （基本用户密钥）密码，然后单击 **Next （下一步）**。
44. 单击 **Next （下一步）**确认设置，并接受恢复数据时所对应的默认位置。

执行步骤 45 到 49，重新安装原来的基本用户配置。

45. 选择适当的安全保护功能，然后单击 **Next （下一步）**。
46. 单击适当的电子邮件客户端，将其选中后单击 **Next （下一步）**。
47. 单击加密证书，然后单击 **Next （下一步）**进行应用。
48. 单击 **Next （下一步）**确认设置。
49. 单击 **Finish （完成）**。
50. 重新启动计算机。

注意：保护 Basic User （基本用户）密码。**没有此密码，就不能访问或恢复加密数据。**

驱动器锁

驱动器锁是一种行业标准的安全保护功能，可防止他人擅自访问多功能插槽硬盘驱动器上的数据。驱动器锁已成为 Computer Setup （计算机设置）实用程序的补充功能。只有检测到支持驱动器锁的硬盘驱动器时，才能利用这种功能。

驱动器锁是为那些极其关注数据安全的 HP 客户提供的。对于这些客户而言，与他人擅自访问其数据内容造成的损失相比，硬盘驱动器的成本以及丢失其中的数据所造成的损失是无足轻重的。为了既能够达到所需的安全保护级别，又能够解决忘记密码的实际问题， HP 提供的驱动器锁实施了双重密码保护方案。其中的一个密码由系统管理员设置和使用，另一个密码则通常由最终用户设置和使用。如果两个密码都丢失了，则没有任何方法能够解除对驱动器的锁定。因此，在公司信息系统上复制硬盘驱动器中含有的数据或者定期备份时，使用驱动器锁最安全。

如果两个驱动器锁密码都丢失了，硬盘驱动器便无法使用了。对于不符合先前介绍的客户情况的用户而言，这可能是无法承受的风险。对于符合上述客户情况的用户而言，考虑到硬盘驱动器上所存储的数据的性质，或许能够承受这种风险。

使用驱动器锁

DriveLock （驱动器锁）选项位于 Computer Setup （计算机设置）实用程序的 Security （安全保护）菜单上。用户可利用所显示的选项来设置主人密码或启用驱动器锁。要启用驱动器锁，就必须输入用户密码。由于驱动器锁的初始配置通常是由系统管理员设置的，所以应该先设置主人密码。无论系统管理员准备启用还是禁用驱动器锁， HP 均鼓励系统管理员设置主人密码。这样一来，即使将来驱动器被锁定，管理员也能够修改驱动器锁的设置。一旦设置了主人密码，系统管理员就可以启动或禁用驱动器锁。

如果硬盘驱动器被锁定，系统便会在开机自测时要求用户输入密码以解除对设备的锁定。如果设置了开机密码，而且该密码与设备的用户密码一致，那么开机自测时便不再提示用户重新输入该密码。否则，系统会提示用户输入驱动器锁密码。此时，

既可以输入主人密码，也可以输入用户密码。用户有两次机会来输入正确的密码。如果两次尝试均告失败，系统便会继续进行开机自测，但用户将无法访问该驱动器。

驱动器锁的应用

在公司环境中，系统管理员为用户提供多功能插槽硬盘驱动器，以便在某些计算机上使用。驱动器锁安全保护功能在这种环境下得到广泛应用。系统管理员应负责配置多功能插槽硬盘驱动器，其中就涉及到设置驱动器锁的主人密码。万一用户忘记了用户密码或者将该设备交给另一位员工使用，就可以始终利用主人密码重新设置用户密码，进而重新获得访问硬盘驱动器的权限。

如果公司的系统管理员选择启用驱动器锁， HP 则建议公司也制定设置和维护主人密码的公司策略。这样做可防止出现以下情况：员工在离开公司前有意或无意地设置了两个驱动器锁密码。出现这种情况后，硬盘驱动器就变得毫无用处，只能更换硬盘驱动器。同样，由于没有设置主人密码，系统管理员会发现他们自己也无法使用硬盘驱动器，而且无法定期检查未授权的软件、其它资产控制功能以及支持功能。

对于安全保护要求不严格的用户而言， HP 不主张他们启用驱动器锁。此类用户包括个人用户或者并不对其硬盘驱动器上的敏感数据进行日常维护的用户。对于这些用户而言，遗忘两个密码对硬盘驱动器造成的潜在损失要比驱动器锁保护的数据的价值高得多。设置密码可用来限制对 Computer Setup （计算机设置）实用程序和驱动器锁的访问。系统管理员只需指定设置密码，并且不让最终用户知道该密码，即可限制用户启用驱动器锁。

智能机盖传感器

只有某些机型提供了智能机盖传感器，它结合了软硬件技术，一旦有人卸下了计算机机盖或侧面板，就会发出警报。如下表所述，智能机盖传感器的保护级别有三种。

智能机盖传感器的保护级别

级别	设置	说明
级别 0	禁用	禁用智能机盖传感器 （默认设置）。
级别 1	通知用户	计算机重新启动后，屏幕上将显示一则信息，说明曾经有人卸下计算机机盖或侧面板。
级别 2	设置密码	计算机重新启动后，屏幕上将显示一则信息，说明曾经有人卸下计算机机盖或侧面板。您必须输入设置密码才能继续执行以后的操作。

使用 Computer Setup （计算机设置）实用程序可以更改上述设置。有关 Computer Setup （计算机设置）实用程序的详细信息，请参阅*计算机设置 (F10) 实用程序指南*。

设置智能机盖传感器的保护级别

要设置智能机盖传感器的保护级别，请完成以下各步操作：

1. 打开或重新启动计算机。如果在 Windows 中，请单击 **Start （开始） > Shut Down （关闭系统） > Restart the Computer （重新启动计算机）**。
2. 当显示器指示灯变成绿色时，立即按下 **F10** 键。您也可以根据需要按下 **Enter** 键跳过标题屏幕。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

3. 选择 **Security （安全保护）**，然后选择 **Smart Cover （智能机盖）**，并按照屏幕上的说明进行操作。
4. 在退出之前，请单击 **File （文件） > Save Changes and Exit （保存更改并退出）**。

智能机盖锁

某些型号的 HP 计算机上配备了智能机盖锁，这是一种可由软件控制的机盖锁。该锁可防止他人擅自接触计算机的内部组件。计算机出厂时智能机盖锁并未处于锁定位置。

注意：为了最大限度地确保机盖锁的安全性，请务必设定设置密码。设置密码可防止他人擅自访问 Computer Setup （计算机设置）实用程序。

只有某些系统提供智能机盖锁选件。

锁定智能机盖锁

要激活并锁定智能机盖锁，请完成以下各步操作：

1. 打开或重新启动计算机。如果在 Windows 中，请单击 **Start （开始） > Shut Down （关闭系统） > Restart the Computer （重新启动计算机）**。
2. 当显示器指示灯变成绿色时，立即按下 **F10** 键。您也可以根据需要按下 **Enter** 键跳过标题屏幕。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

3. 选择 **Security （安全保护）**，然后选择 **Smart Cover （智能机盖）**和 **Locked （锁定）**选项。
4. 在退出之前，请单击 **File （文件） > Save Changes and Exit （保存更改并退出）**。

解除对智能机盖锁的锁定

1. 打开或重新启动计算机。如果在 Windows 中，请单击 **Start（开始） > Shut Down （关闭系统） > Restart the Computer（重新启动计算机）**。
2. 当显示器指示灯变成绿色时，立即按下 **F10** 键。您也可以根据需要按下 **Enter** 键跳过标题屏幕。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

3. 选择 **Security （安全保护） > Smart Cover （智能机盖） > Unlocked （解除锁定）**。
4. 在退出之前，请单击 **File （文件） > Save Changes and Exit（保存更改并退出）**。

智能机盖防故障钥匙的用途

如果启用了智能机盖锁，却不能输入相应的密码来禁用该锁，就必须用一把智能机盖防故障钥匙来开启计算机机盖。遇到下面任何一种情况都需要使用智能机盖防故障钥匙：

- 断电
- 启动失败
- PC 组件 （如处理器或电源）故障
- 忘记了密码

注意：智能机盖防故障钥匙是 HP 提供的专用工具。应备有此钥匙；可向授权的经销商或服务供应商订购一把以备不时之需。

按照下列某种方式订购防故障钥匙：

- 与 HP 授权经销商或服务供应商联系。
- 拨打保修声明中列出的相关电话号码。

有关使用智能机盖防故障钥匙的详细信息，请参阅 *硬件参考指南*。

主引导记录安全保护

主引导记录 (MBR) 中含有通过磁盘成功引导，以及访问磁盘上存储的数据所需的信息。主引导记录安全保护功能可以防止无意或恶意地更改主引导记录。例如，因某些计算机病毒或磁盘实用程序使用不当而导致主引导记录发生变化。如果重新启动系统后发现主引导记录已发生变化，还可以利用主引导记录安全保护功能来恢复 “最新最全”的主引导记录。

要启用主引导记录安全保护，请完成以下各步操作：

1. 打开或重新启动计算机。如果在 Windows 中，请单击 **Start（开始） > Shut Down （关闭系统） > Restart the Computer（重新启动计算机）**。
2. 当显示器指示灯变成绿色时，立即按下 **F10** 键。您也可以根据需要按下 **Enter** 键跳过标题屏幕。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

3. 选择 **Security （安全保护） > Master Boot Record Security（主引导记录安全保护） > Enabled （启用）**。
4. 选择 **Security （安全保护） > Save Master Boot Record （保存主引导记录）**。
5. 在退出之前，请单击 **File （文件） > Save Changes and Exit（保存更改并退出）**。

一旦启用了主引导记录安全保护，那么无论处于 MS-DOS 还是 Windows 安全模式下， BIOS 都可以防止对当前可引导磁盘的主引导记录做任何更改。

大多数操作系统都控制对当前可引导磁盘的主引导记录的访问； BIOS 无法防止操作系统在运行时发生变化。

每次打开或重新启动计算机时， BIOS 都会将当前可引导磁盘的主引导记录与先前保存的主引导记录作比较。如果检测到更改，而且当前的可引导磁盘正是先前保存主引导记录的磁盘，屏幕上会显示以下信息：

1999 — Master Boot Record has changed （主引导记录已更改）

Press any key to enter Setup to configure MBR Security。（按任意键进入 Setup （计算机设置）实用程序以配置主引导记录安全保护。）

一旦进入 Computer Setup （计算机设置）实用程序，必须执行以下操作：

- 保存当前可引导磁盘的主引导记录；
- 恢复先前保存的主引导记录；或者
- 禁用主引导记录安全保护功能。

如果已设定了设置密码，就必须知道该密码。

如果检测到更改，而且当前的可引导磁盘并**不是**先前保存主引导记录的磁盘，屏幕上会显示以下信息：

2000 — Master Boot Record Hard Drive has changed （主引导记录硬盘驱动器已更改）

Press any key to enter Setup to configure MBR Security。（按任意键进入 Setup （计算机设置）实用程序以配置主引导记录安全保护。）

一旦进入 Computer Setup （计算机设置）实用程序，必须执行以下操作：

- 保存当前可引导磁盘的主引导记录；或者
- 禁用主引导记录安全保护功能。

如果已设定了设置密码，就必须知道该密码。

万一破坏了先前保存的主引导记录，屏幕上会显示以下信息：

1998 — Master Boot Record has been lost （主引导记录已丢失）

Press any key to enter Setup to configure MBR Security。（按任意键进入 Setup （计算机设置）实用程序以配置主引导记录安全保护。）

一旦进入 Computer Setup （计算机设置）实用程序，必须执行以下操作：

- 保存当前可引导磁盘的主引导记录；或者
- 禁用主引导记录安全保护功能。

如果已设定了设置密码，就必须知道该密码。

对当前的可引导磁盘进行分区或格式化之前所作的准备工作

在更改当前可引导盘的分区或对其进行格式化之前，确保已禁用了主引导记录安全保护功能。 FDISK 和 FORMAT 等磁盘实用程序会尝试更新主引导记录。如果在更改磁盘的分区或对其进行格式化之前启用了主引导记录安全保护，您可能会收到磁盘实用程序发出的错误信息，或者在下次打开或重新启动计算机时收到主引导记录安全保护的警告。要禁用主引导记录安全保护，请完成以下各步操作：

1. 打开或重新启动计算机。如果在 Windows 中，请单击 **Start （开始） > Shut Down （关闭系统） > Restart the Computer （重新启动计算机）**。
2. 当显示器指示灯变成绿色时，立即按下 **F10** 键。您也可以根据需要按下 **Enter** 键跳过标题屏幕。

如果未能及时按下 **F10** 键，就必须关闭计算机，然后重新打开，再次按下 **F10** 键，才能访问该实用程序。

3. 选择 **Security （安全保护） > Master Boot Record Security （主引导记录安全保护） > Disabled （禁用）**。
4. 在退出之前，请单击 **File （文件） > Save Changes and Exit （保存更改并退出）**。

缆锁装置

您可以在计算机背面板上安装缆锁，以便将计算机固定在工作区内。

有关图解说明，请参阅*文档库*光盘中的*硬件参考指南*。

指纹识别技术

HP 指纹识别技术不仅提高了网络安全性能、简化了登录过程，而且减少了管理公司网络的相关费用。有了它，用户不必再输入用户密码。该技术价位合理，不再仅仅适合那些高科技和高度安全的企业使用。

对指纹识别技术的支持因机型而异。

有关详细信息，请访问：

http://h18000.www1.hp.com/solutions/security。

故障通知和恢复

故障通知和恢复功能结合了创新的硬件和软件技术，不仅可以防止丢失重要的数据，而且能够将意外停机的次数降到最低。

如果出现故障，计算机会显示本地警报信息，其中指明所发生的故障和建议采取的措施。接下来，您可以使用 HP Client Manager （HP 客户机管理器）来查看系统当前的运行状况。如果计算机与 HP Insight Manager （HP 洞察管理器）、 HP Client Manager （HP 客户机管理器）或其它系统管理应用程序管理的网络相连，计算机还会向相应的网络管理应用程序发送故障通知。

驱动器保护系统

驱动器保护系统 (Drive Protection System, DPS) 是一个诊断工具，内置于某些 HP 计算机上安装的硬盘驱动器中。 DPS 是专门设计的一个工具，有助于诊断因换用了无保证的硬盘驱动器而引起的问题。

HP 在生产计算机时，已使用 DPS 对每个安装的硬盘驱动器进行了测试，并且将重要信息的记录永久地写入了驱动器中。每次运行 DPS 时，都会将测试结果写入硬盘驱动器中。服务提供商可以利用此类信息，帮助您诊断是何种状况致使您运行 DPS 软件。有关使用 DPS 的说明，请参阅*故障排除指南*。

耐电涌电源

当计算机受到无法预料的电涌冲击时，集成的耐电涌电源可提高计算机的可靠性。此电源在额定情况下可承受高达 2000 伏的电涌冲击，而不会导致系统停机或数据丢失。

热感器

热感器是一种跟踪记录计算机内部温度的硬件和软件功能。如果温度超出了正常范围，此功能便会显示警告信息，使您能够在内部组件受损或数据丢失之前及时采取措施。

索引